Book Chapter

Cyber-Attack Research for Integrated Energy Systems by the Correlated Matrix Based Object-Oriented Modeling Method

Heqin Tong[1,2,3]*, Jianbing Xu[1,2,3], Xiao Li[1,2,3] and Liquan Zhang[1,2,3]

[1]State Grid Electric Power Research Institute, China
[2]NARI Group Corporation, China
[3]NARI Technology Co., Ltd., China

***Corresponding Author:** Heqin Tong, State Grid Electric Power Research Institute, Nanjing, China

Published **January 12, 2023**

This Book Chapter is a republication of an article published by Heqin Tong, et al. at Frontiers in Energy Research in August 2022. (Tong H, Xu J, Li X and Zhang L (2022) Cyber-attack research for integrated energy systems by the correlated matrix based object-oriented modeling method. Front. Energy Res. 10:774645. doi: 10.3389/fenrg.2022.774645)

How to cite this book chapter: Heqin Tong, Jianbing Xu, Xiao Li, Liquan Zhang. Cyber-Attack Research for Integrated Energy Systems by the Correlated Matrix Based Object-Oriented Modeling Method. In: Advances in Energy Research: 4th Edition. Hyderabad, India: Vide Leaf. 2023.

© The Author(s) 2023. This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Conflict of Interest: HT, JX, XL, and LZ were employed by State Grid Electric Power Research Institute, NARI Group Corporation, and NARI Technology Co., Ltd.

Author Contributions: HT was responsible for proposing the modeling method and the specific work of this paper. JX, XL and LZ carried out some of the calculation work.

Funding: The authors declare that this study received funding from National Natural Science Foundation of China-State Grid Corporation of China Joint Found Project (No. U1866209). The funder was not involved in the study design, collection, analysis, interpretation of data, the writing of this article or the decision to submit it for publication.

Data Availability Statement: The original contributions presented in the study are included in the article/Supplementary Material; further inquiries can be directed to the corresponding author.

Abstract

The rise of integrated energy system requires the integration of multiple sources of energy to be embraced and transit over power grid, that means the information and communication system of traditional power system will be extended, and their complexity will be increased. As the information and communication system plays a more important role in the infrastructure of power system, cyber-attack on them may impact on the power system and cause serious threat to the integrated energy system. To analyze the threat on the complex and integrated system, some researchers provide some modeling methods to study the impact of cyber-attack on the information and communication system, such as Attack Tree Model, Attack Graph Model, Petri Net Model for cyber-attack, Attack Description Language Model, State Transition Graph Model, etc. However, these modeling methods have some shortcomings, for example, they cannot describe the systematical cyber-attack and show the secure status during the cyber-attack; it is hard for them to analyze the larger and complicated information and

communication system. To overcome the shortages, in this paper, a correlated matrix based object-oriented model is proposed for cyber-attack modeling. With this model, the relationship between the attacker and victim can be directly built; the cyber-attack path and packet from the attacker can be tracked; and the status of the nodes and links can be showed during cyber-attack. There are two steps to build the cyber-attack model. Firstly, the procedure and approach of the cyber-attack will be modeled by an object-oriented method; then, correlated matrix model will be built for network topology, attack path and attack procedure. By combining these two models, the whole cyber-attack model is created. Finally, to demonstrate the modeling method and its benefit, we use the MITM (Man-in-the-middle Attack) attack on measurement data of AVC (Automation Voltage control) system as examples, and build hardware-in-the-loop (HIL) co-simulation platform to verify the model.

Keywords

Integrated Energy System; Object-Oriented Method; Correlation Matrix; Cyber-Attack; Automation Voltage Control System

Introduction

The increasingly usage of multiple source of energy, such as renewable energy and distributed energy, leads to the instability of energy utilization and energy supply [1], which puts forward higher requirements for data acquisition and control system. Due to the measurement and control mechanism increasingly depending on the information and communication system [2,3], the tight interdependence between communication and integrated energy system makes it more vulnerable to the cyber-attacks [4], especially for the power system. Hackers' attacks on communication and information system can directly or indirectly affect the measurement and control of power system, further affect the safe and stable operation of power system, and even lead to large-scale power outage.

Therefore, the security of network and information system has attracted more and more attention all over the world. Facing to the endless cyber-attack cases, it is difficult for administrator to analyze and predict the impact of endless cyber-attack means on the network only by the research of individual cyber-attack behavior. Thus, it is necessary to model the overall situation and attack process on the network, predict the possible path and probability of cyber-attack, and realize the security assessment of network state, provide reference for safety measures. At present, many modeling methods for cyber-attacks have been proposed, including attack language, attack tree, attack graph, state transition graph, etc., and these methods have their respective advantages and disadvantages as following:

(1) Attack tree model: a tree structure is used to describe the attack on the system. The total target of the attack is regarded as the root node of the tree, and the sub target of the total target is regarded as the sub node. Each path from the root node to the leaf node represents a complete attack process to achieve the attack target. For example, the paper [5] proposes to build attack tree model in a recursive or progressive way to directly show the attack steps of attackers. In reference [6], the attack tree modeling method is used to analyze the impact of SCADA oriented network attacks on power system. However, the attack tree is limited to description and formal analysis, which is too subjective, and its scale problem makes it not suitable for large-scale network environment.
(2) Attack graph model: it is composed of a set of attack plans that attackers can destroy the network system by simulating attacks on existing security vulnerabilities and finding all attack paths that can reach the target [7]. Compared with attack tree and Petri net, attack graph is more powerful in describing network attack process. Through the attack graph, we can show how an attacker attempts to invade the communication or information system from the initial state to the target state. A complete attack graph is a possible operation sequence to reach the target. For example, in reference [8], based on the improved attack graph algorithm, the cross space cascading fault assessment of power

information physical system is realized; in reference [9], a dynamic risk assessment model is proposed based on the Bayesian attack graph with the atomic attack probability calculation; and in reference [10], the forward risk probability update algorithm and the forward-backward combined risk probability update algorithm is introduced to improve the attack graph model to reflect the real-time network attack events. There are two kinds of typical attack graph generation method: one is state transition, which can generate complete attack graph by algorithm, but it often causes "state space explosion" in large-scale commercial network; the other is host centric, which can be used in large-scale network, but its disadvantage is that it can't list the all attack paths.

(3) Attack network model based on Petri Net: it is composed of location, transition, arc and token. The location corresponds to the nodes in the attack network, and the attack behavior is described by the transition of token between locations. This method is preferable to represent the state, the action and the progress of the attack. For example, Steffan comprehensively uses graph theory, Petri net and other technologies to describe network attacks, and expounds the correlation of cyber-attacks [11]. In reference [12], Petri net is used to model and analyze the network penetration attack testing process. In reference [13], the stochastic Petri net based model is used to analyze the topology attacks on the power system. In reference [14], a novel Cyber Physical Defense Framework is proposed to analyze and deal with the cyber-attack on smart grid by the hierarchical Petri Net model and recovery method. However, due to the limitation of scale, it is difficult to analyze the communication and information system with large scale and complex network topology.

(4) Network Attack Language: it is the earliest modeling method to describe network attack. It describes network attack through a formal description language, including NASL (Nessus Attack Scripting Language), STATL (State/Transition-based Attack Description Language), and object-oriented language modeling, etc., which directly describes one or a category of attack behavior. For example,

in reference [15], STATL language is used to describe the attack behavior by state and state transition; in reference [16], STATL language is used to provide intrusion feature library for network intrusion detection system; and in reference [17], object-oriented method and AKDL (Attack Knowledge Description Language) language is used to realize attack knowledge modeling for security defense system. The method of network attack language is suitable for engineering application, but it is not suitable for describing staged attack behavior, nor can it show the security situation of the whole communication and information system.

(5) State transition graph modeling: this modeling method is based on the finite state machine model to represent the attack process. The intrusion process of attackers can be regarded as the procedure of improving their operation authority by taking advantage of the vulnerabilities and misconfigurations in the communication and information systems. For example, in reference [18], an attack graph construction method based on intelligent state transition and authority improvement is proposed to realize the analysis of large-scale complex network attacks; in reference [19] and [20], the author provides Hidden Markov Model based model (HMM-based) to detect distributed denial of service (DDoS) attack. However, this model only describes the state transition in the specific node, but the whole network is ignored. Moreover, the state in this model is only a symbol, and its meaning is not clear [21].

As more and more distributed energy resources from different energy networks are integrated through the power system, a large number of distributed sensors and controllers for the distributed energy resources will be introduced, which rapidly increases the diversity and complexity of the communication network [22]. To analyze the cyber-attacks and security situation for this complex network, the network topology, attack path and attack behavior should be considered in the cyber-attack model. However, the traditional modeling methods mentioned above show a lack of the description of network topology and the attack path, which makes it difficult to find out the potential security problems in a

network or estimate the security situation of the network when a cyber-attack occurs. Thus, this paper provides a new method of the correlated matrix based object-oriented modeling method to solve this drawback. The main features and contributions of this modeling method are as follows.

1) By applying the object-oriented analysis method, we can directly display the relationship between the attacker and the attacked object, and show the possible attack path.
2) The topology of communication and information network can be described by the correlated matrix, which provides an effective way for analyzing the transmission path of attack packets.
3) The status of the nodes and links during cyber-attack can be displayed, which help us evaluate the impact of cyber-attack.

To introduce the modeling method, this paper is organized as follows. Firstly, the background and traditional modeling methods are introduced; then, the definition and modeling process of the correlated matrix based object-oriented modeling method is provided; after that, scenario of the MITM (Man in the Middle Attack) attack is applied to demonstrate how to use the modeling method; to validate the MITM attack model, we build a hardware-in-the-loop (HIL) co-simulation platform to emulate the MITM attack on the real route and study the impact on power system; finally, we conclude this paper.

Object-Oriented Modeling for Cyber-Attack

The model of cyber-attack is an abstract description of the security problems existing in the network, the process of attack behavior, and the attack rules and approaches applied by the attacker. It describes the premise, target, consequence and other characteristics of the attack process; identifies the relationship among the vulnerabilities from the perspective of attack; describes the attack path of the attacker; and provides a reference for the formulation of system protection measures.

The object-oriented method is a way to understand and describe the objective world. The characteristic of this method is that the

attributes describing the static characteristics of things and the operations representing their dynamic behaviors are put together as a whole, and an objective world model can be established with limited steps [23]. It plays an important role in the field of computer science and information technology because its characteristics are consistent with the thinking method of human habits [23].

Due to the characteristics of network attack behavior, the model constructed by object-oriented can clearly describe the method and process of network attack. At the same time, it can also show the system vulnerability intuitively to a network security administrator, and trace the steps of the attacker successfully attacking the system. It provides an effective method for network security administrator to discover attack behavior and improve system security.

Basic Concepts

When using object-oriented method to model the attack of communication information system, it is necessary to abstract the real system and define some basic concepts.

Definition 1: Network object (N): the instance of communication link or information node is encapsulated as a network object, which can be a communication node in the communication and information system, such as router, switch, SDH (Synchronous Digital Hierarchy) equipment, etc., or a communication link between communication nodes, such as optical fiber link, wireless communication link, etc., or a substation or data center as a system level abstraction;

Definition 2: Attribute of network object, or network attribute (A): network attribute is the representation of the state characteristics of the object being attacked, including service, vulnerability, bandwidth, hardware resources, system version, etc. Attribute of network object can be identified by $<N, V>$ tuple, where N is the name of the attribute, V is the specific value for the attribute, which is identified by 0, 1 and -1. 0 means that the object has no corresponding attribute, 1 indicates that the

attribute of the component is not exploited by the attacker, -1 indicates that the attribute of the component has been exploited by the attacker;

Definition 3: Method of network object, or network method (M): network method is defined as the method for network object to process the received packet or user operation request, and it can also be defined as the processing method of attack behavior, such as refusal reply for port scanning behavior, packet filtering, etc.; Network method can be represented by ＜N, V＞ tuple, in which N represents the name of the method, V represents the specific value of N by 0, 1 and - 1, where 0 means that the method does not exist, 1 means that the method is valid, and -1 means that the method has been used by an attacker;

Definition 4: Attack behavior object (ON): by encapsulating the attack instance into an attack behavior object, it can be represented as a single attack or a compound attacks. A successful attack behavior will change the attributes of one or more network objects;

Definition 5: Attack Attribute (OA): attack attribute defines the operation of an attack behavior object. As the precondition, when one or more attack attributes are fully satisfied, the attack action will be trigged. The attack attribute can be identified by ＜N, V＞ tuple, where N is the name of the attribute, V is the specific value for the attribute, which is identified by 0 and -1, where 0 means that the attribute of attack behavior is ineffective and -1 means that the attribute of attack behavior is effective;

Definition 6: Attack method (OM): attack method is the description of the attack action of the attack behavior object. When the premise of meeting the attack behavior attribute, one or more attributes of the network object will be modified by attack method to complete the attack action. Attack method can be identified by ＜N, V＞ tuple, where N is the name of the method, V is the specific value of the method, which is identified by 0 and - 1, where 0 means the method is ineffective and -1 means the attack method is effective;

Definition 7: Class (C): a class is a collection of similar objects with the same name, relationship, attribute and method. According to different objects, they can be divided into communication link classes, communication node classes, communication and information node classes, attack behavior classes, attack (transit) path classes, etc.

Representation of Model

When the object-oriented method is used to model the attack on communication and information system, the attack process can be abstracted as the object of communication and information system changing from initial state to the target state after the operation performed by the attack behavior object. And the attack behavior can also be regarded as the operation process on the network object for changing its attributes.

The attack behavior is encapsulated in the attack object, whose attribute OA is used to describe the target and the operations on the attacked object. The target of the attack is a set of state changes, which indicates the possibility that the attribute A of the network object may be changed after the attack. For example, the buffer overflow attack can enable the attacker to obtain privileges from the network object, or implant Trojans in the network object, or maybe not cause any consequences.

The operation process of the attack behavior is identified by the attack method OM, such as scanning port and vulnerability of the network object to determine whether the attack can be launched. On the other hand, the network method M defines the protection method for the network object, such as packet filtering, preventing packets from the specific port, etc.

Instance of Modeling

Take an attack on a router as an example: the attacker discovers a router by scanning, and remotely attacks on it with open remote login permission, brutally breaks the login password of the router by using the password guessing attack method, and then remotely launches in the router and modifies the routing

table configuration to complete the attack on the router. The object-oriented method for cyber-attack modeling is shown in Figure 1.

As shown in Figure 1, router N_1 contains attributes A_1^0 of remote login, and A_2^0 of routing table, and attack behavior ON_1 contains attack methods OM_1 of remote login password guessing attack, and OM_2 of modifying routing table. If the prerequisite of the attribute A_1^0 matching the method OM_1, the attacker will change the attribute A_1^0 to attribute A_1^1 of the attacker's login; due to the prerequisite of the attribute A_1^1, the attacker tries to change the attribute A_2^0 by the method OM_2. If the attribute A_2^0 matches the attack method OM_2, the routing table will be modified, and the attribute A_2^0 will be change to the attribute A_2^1.

Matrix Modeling of Network Attack

Object-oriented network attack modeling methods can be described by a formal specification language or knowledge description language (/knowledge base). Although these methods can effectively show the attack means, the system weaknesses, and the consequences of the attack, they have some limitations to describe the network attack on a complex communication and information system, such as the transmission path of attacker's packets in the network, the role of each intermediate node in the attack process, and the impact of topology on the attack effect. Therefore, designing a network attack model that can describe the topology of communication information system is an important extension for the existing attack model.

This paper proposes a correlated matrix based object-oriented modeling method for cyber-attack modeling and analysis, which extends the object-oriented modeling method for network attack, and effectively describes the evolution process of a communication and information network from the initial state to the state after several different attacks.

The modeling process for cyber-attack is as follows: firstly, communication and information network is modeled in a matrix; then, considering with the topology of communication and

information network, the cyber-attack is modeled in matrix; based on that, by iterated logical matching between the matrix of communication and information network and the matrix of cyber-attack, the network attack process will be represented, and the final status matrix of communication and information network is generated.

Take a communication and information system with eight communication and information nodes and nine full duplex communication links as an example to illustrate the modeling process for the cyber-attack. The topology of communication information network is shown in Figure 2.

Matrix Modeling of Communication Information Network

Definition 8: Matrix of communication network object: the attributes and methods of the network object N can be identified by matrix [A M]. A is the vector set of network attributes, which may contain link bandwidth, CPU performance, memory, remote login and services, etc.; M is the vector set of object methods, which may contain password protection for remote login, the specific data filtering, viruses protection, etc.

Based on the node and link model, a communication network object correlated matrix N (Network) with 26 communication information object elements is established to describe the topology and characteristics of the communication system. The matrix N is a large sparse matrix, whose structure is shown in equation 1.

The 8 × 8 matrix N can describe the state of each object element in the whole communication network. Where: N_{ij} = [A M], if i = j, then N_{ij} represents a communication or information node in the communication network; If $i \neq j$, N_{ij} is a unidirectional link from node N_{ii} to N_{jj} in the communication network; If there is no link connecting node N_{ii} to N_{jj}, the corresponding N_{ij} and N_{ji} in the matrix are represented by 0 [24]. The state of the elements in the N matrix is represented by the superscript of the elements. For

example, N_{11}^0 represents the initial state of the object element N_{11}.

$$\mathbf{N} = \begin{pmatrix} \boldsymbol{N_{11}}^{\mathbf{0}} & \cdots & \boldsymbol{N_{i1}}^{\mathbf{0}} \\ \vdots & \ddots & \vdots \\ \boldsymbol{N_{1j}}^{\mathbf{0}} & \cdots & \boldsymbol{N_{ij}}^{\mathbf{0}} \end{pmatrix} \quad (1)$$

Matrix Modeling of Attack (Behavior) Object

Definition 9: Matrix of attack behavior object: the attributes and methods of attack behavior object ON can be identified by matrix [OA OM]. OA is the vector set of attack attributes, which may contain attacking port number, attacking IP address, number of attack packets, etc. OM is the vector set of attack methods, which may include consumption of link bandwidth, consumption of system resources, modification of configuration information, planting of Trojans, etc.

Similar to the matrix modeling of communication and information network, the matrix modeling of cyber-attack can be established for the attack behavior on the communication and information network with eight communication or information nodes and nine communication links through the matrix modeling, and the attack path, attack method and attack process can be described by the attack object correlated matrix ON (Operating Network). In the ON matrix, the attack sequence is represented by the superscript of the attack object ON. For example, ON^0_{33} represents the first attack on the N_{33} object element. The structure of the attack object matrix is shown in equation 2.

$$\mathbf{ON} = \begin{pmatrix} \boldsymbol{ON_{11}}^{\mathbf{0}} & \cdots & \boldsymbol{ON_{i1}}^{\mathbf{0}} \\ \vdots & \ddots & \vdots \\ \boldsymbol{ON_{1j}}^{\mathbf{0}} & \cdots & \boldsymbol{ON_{ij}}^{\mathbf{0}} \end{pmatrix} \quad (2)$$

The ON matrix is also 8 ×8. The elements in the matrix can describe the path and method of the attacker attacking the target object through the nodes and links of the communication network. Where: ON_{ij} = [OA OM], if i = j, ON_{ij} represents an

attack on a communication information node in the communication network or the attack packet passing through; If the attack object ON_{ij} does not exist, or the attack packet does not pass through the object, the corresponding ON_{ij} in the matrix is represented by 0 [24]. if $i \neq j$, ON_{ij} represents that the attacker attacks a unidirectional link from N_{ii} to N_{jj} in the communication network or uses this link to transit attack packet to the target object; If the attacker neither attack nor use the link from the N_{ii} to N_{jj}, the corresponding ON_{ij} and ON_{ji} in the matrix are represented by 0 [24].

Matrix Modeling and Analysis of Attack Process

In Section 3.1 and 3.2, the communication and information system network model and cyber-attack model are established. Based on this, the attack process correlated matrix model is established. Through the model, the process and path of network attack and the probability of attack success are described; at the same time, it can also describe the state changes of communication and information nodes after network attacks, and provide the corresponding association model for the analysis and modeling for the network attacks. The modeling framework and analysis process for the network attack can be represented in Figure 3.

In the diagram, the occurrence and duration of the cyber-attack can be represented by a pure delay component e^{-T1S1}, where T1 represents the time when the network attack occurs and S1 represents the duration of the attack. Considering that the cyber-attack on the target system is step by step, multiple interactions between the communication information network matrix model and the attack matrix model are designed for the modeling. The logical relationship of the interaction is mainly represented in the algorithm, which is represented as "⊗" shown in Figure 3.

Definition 10: Logical relation (⊗): it describes the logical operation between the elements of attack behavior object and network object, including the logical matching between the attribute of attack behavior and the method of network object,

and the logical matching between the method of attack behavior and the attribute of network object.

A simple attack case can illustrate how the logical relation (⊗) works. When the attacker finds the remote router through remote scanning, and logs into its configuration interface by cracking the login password of the router, he can modify the router's routing table, configure a packet forwarding route for the specific IP address and port number, so that the relevant packets will be forwarded to the attacker; then the attacker tampers the packets and sends them back to the corresponding router, and the router forwards the tampered packets to the target communication information node, so as to complete the MITM attack process. The matrix modeling of attack process is shown in equation 3. The logic matching rules for each vector in the matrix model are as follows:

1. When matching the attack behavior object ON_{ij} and the network object N_{ij}, logical matching between the OA of the object ON_{ij} and the M of the object N_{ij} is performed first. If a method M_i matches an attack attribute OA_i, the attack behavior will be filtered; on the contrary, the attack behavior will be effective;
2. If the attack behavior is effective, logical matching between the OM of the object ON_{ij} and A of the object N_{ij} will be performed, which means that the attack method operates on the attribute of the network object. If it is effective, the attribute A of the object N_{ij} will be modified, and the attack will be successful; on the contrary, the attribute A of object N_{ij} is not modified, and the attack fails or the attack can utilize the attribute.

$$N^2 = \begin{pmatrix} N_{11}^{\,0} & N_{12}^{\,0} & 0 & 0 & 0 & 0 & 0 & 0 \\ N_{21}^{\,0} & N_{22}^{\,0} & N_{23}^{\,0} & N_{24}^{\,0} & 0 & N_{26}^{\,0} & 0 & 0 \\ 0 & N_{32}^{\,0} & N_{33}^{\,0} & 0 & 0 & 0 & 0 & 0 \\ 0 & N_{42}^{\,0} & 0 & N_{44}^{\,0} & N_{45}^{\,0} & 0 & 0 & 0 \\ 0 & 0 & 0 & N_{54}^{\,0} & N_{55}^{\,0} & 0 & N_{57}^{\,0} & N_{58}^{\,0} \\ 0 & N_{62}^{\,0} & 0 & 0 & 0 & N_{66}^{\,0} & N_{67}^{\,0} & 0 \\ 0 & 0 & 0 & 0 & N_{75}^{\,0} & N_{76}^{\,0} & N_{77}^{\,0} & N_{78}^{\,0} \\ 0 & 0 & 0 & 0 & N_{85}^{\,0} & 0 & N_{87}^{\,0} & N_{88}^{\,0} \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & ON_{22}^{\,0} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & ON_{32}^{\,0} & ON_{33}^{\,0} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot e^{-S0 \cdot T0}$$

$$\otimes \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & ON_{22}^{\,1} & 0 & ON_{24}^{\,1} & 0 & 0 & 0 & 0 \\ 0 & ON_{32}^{\,1} & ON_{33}^{\,1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & ON_{44}^{\,1} & ON_{45}^{\,1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & ON_{55}^{\,1} & 0 & 0 & ON_{58}^{\,1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & ON_{88}^{\,1} \end{pmatrix} \cdot e^{-S1 \cdot T1} \quad (3)$$

Modeling Examples

Scenario of the MITM Attack on AVC Measurement

The AVC control runs in the power dispatching data network. Based on the communication network topology in Figure 2, a simple AVC control communication network is shown to illustrate the modeling process in Figure 4. The dotted line represents the normal data path for the measured data and the AVC control command. The red dotted line represents the process of modifying the routing table after the attacker invades the router, so that the measured data returns to the normal routing path via the tampered routing path. In this case, the attacker only modifies the upstream data for measurement, and does not modify the downstream data for AVC control command.

When the communication network is normal, the AVC control center collects the power measurement information from the power measurement node every 5 seconds. By calculation, the AVC control center sends the corresponding voltage regulation value to the corresponding generator unit through the communication special line. Generally, the transmission path of the measurement information starts from the power measurement node via the CE (Customer Edge) router to connect the core network of power dispatching via the PE (Provider Edge) router, and then connects to the AVC control center through the opposite end router. After receiving the measurement data, AVC control center will send the voltage regulation to each generator unit through private communication line. If the attacker successfully costs S1 minutes to intrude into the PE router at T1 time, modifies the routing configuration, establishes a bypass routing transmission path filtered based on the IP address and port number of the packet, and forwards the voltage measurement data of the power measurement node to the attacker, the attacker tampers with the normal measurement data by MITM (Man-in-the-middle) attack at T2 time ($T2 > T1 + S1$). The duration of data tampering is S2 minutes ($S2 > 5$ seconds in order to achieve the corresponding attack effect), and the tampered data are returned to the intruded PE router. Then the intruded PE router sends the tampered data to the AVC control

center through the normal path. After receiving the tampered data, the AVC control center will make a wrong judgment, and result in the AVC deficient control or over control while the AVC control channel has not been attacked.

Modeling for the MITM Attack on AVC Measurement

The procedure of modeling for the above network attacks is as follows:

1. Establish the initialization matrix of communication information network according to the topology of communication information system;
2. Establish the matrix of attack behavior object according to the attack target and mode. If the attacker launches attacks on different targets in different time slots, it is necessary to establish different matrix of attack behavior object according to the different attack targets and time slots, and match them with the matrix of communication network object separately according to the time sequence;
3. Based on the communication information network matrix and the attack object matrix, the final state matrix of the communication information network is obtained by using multiple iterative logical matching.

The cyber-attack can be simplified into two processes: the attack on the router and the attack on the transmitted data. In the model, we can simplify the matrix by assuming the power measure node as a part of object N_{11} and the AVC control center as a part of object N_{88}, and the MITM attack model can be represented as equation 3.

Among them, the router's attack object ON_{22}^{0} (the sequence of attack behavior is represented by superscript, ON_{22}^{0} represents the first attack on N_{22} network object, and the sequence number is 0) contains two vectors: the elements of the attack behavior attribute vector OA^{0} include: OA_1^{0} <remote login, -1>, OA_2^{0} <web port login, -1>, OA_3^{0} <forged routing table, -1>, and etc.; the elements of the attack behavior method vector OM^{0} include: OM_1^{0} <login password cracking, -1>, OM_2^{0} <web password

cracking, -1>, OM_3^0 <modify routing table, -1>, and the values of these elements are -1. Since the attack methods and attributes will not change in the attack path, the values of ON_{33}^0, ON_{32}^0 and ON_{22}^0 are the same. The router object N_{22}^0 contains two vectors: the elements of the network object attribute vector A^0 include: A_1^0 <open remote login, 1>, A_2^0 <web login not supported, 0>, A_3^0 <routing table, 1>, and etc.; the elements of the network object method vector M^0 include: M_1^0 <remote login unprotected, 0>, M_2^0 <prohibit web login, 1>, M_3^0 <unprotected routing table, 0>, and etc. The values of OA^0 and OM^0 constitute the attack state matrix of ON_{22}^0, and the values of A^0 and M^0 constitute the network object state matrix of N_{22}^0. By logical matching of ON_{22}^0 and N_{22}^0, the new state of the network object N_{22}^1 is obtained, which is shown in equation 4.

$$N_{22}^0 \otimes ON_{22}^0 = \begin{pmatrix} A_1^0 & M_1^0 \\ A_2^0 & M_2^0 \\ A_3^0 & M_3^0 \end{pmatrix} \otimes \begin{pmatrix} OA_1^0 & OM_1^0 \\ OA_2^0 & OM_2^0 \\ OA_3^0 & OM_3^0 \end{pmatrix} = \begin{pmatrix} A_1^1 & M_1^1 \\ A_2^0 & M_2^0 \\ A_3^1 & M_3^1 \end{pmatrix} = N_{22}^1 \quad (4)$$

The logical matching process and method of the network object N_{22}^0 and the attack behavior object ON_{22}^0 are shown in Figure 5.

According to the matching logic diagram, the attack will change the attribute A_3 of N_{22} (the routing table is modified), and the state of attribute A3 will change from A_3^0 to A_3^1. Similarly, by establishing corresponding logical matches for other elements in the model, the final result of attack modeling on the router can be obtained, which is represented in the modified routing table which belongs to the attribute A_3 of network object N_{22}.

The attack on the transmission data starts from ON_{33}^1 (ON_{33}^1 represents an attack with the attack order of 1 against N_{33} elements), which contains two vectors: the element of the attack behavior attribute vector OA^1 includes: OA_1^1 <tampering with measurement data, - 1>; the element of the attack behavior method vector OM^1 includes: OM_1^1 <normal receiving and sending data, 1>. The router object N_{33}^0 contains two vectors: the elements of the network object attribute vector A^0 include: A_1^0 <measurement data transmission, 1>, and etc.; the elements of the network object method vector M^0 include: M_1^0 <data transmission, 1>, and etc. The values of OA^1 and OM^1 constitute

the attack state matrix of ON_{33}^1, and the values of A^0 and M^0 constitute the network object state matrix of N_{33}^0. By logical matching of N_{33}^0 and ON_{33}^1, the new state of the network object N_{33}^2 is obtained, which is shown in equation 5. Since the attributes and methods of other network objects in equation 3, such as N_{22}^1, N_{44}^0, N_{55}^0 and N_{66}^0, are the same as those of N_{33}^0, and since the attributes and methods of the attack behavior object are the same as those of object ON_{33}^1, the logical matching of the above network objects and attack behavior objects can be represented in equation 5.

$$\mathbf{N_{33}^0 \otimes ON_{33}^1} = (\boldsymbol{A_1^0} \quad \boldsymbol{M_1^0}) \otimes (\boldsymbol{OA_1^1} \quad \boldsymbol{OM_1^1}) = (\boldsymbol{A_1^2} \quad \boldsymbol{M_1^2}) = \mathbf{N_{33}^2} \tag{5}$$

The logical matching process and method of the network object N_{33}^0 and the attack behavior object ON_{33}^1 are shown in Figure 6:

According to the matching logic diagram, the attack will cause the change of attribute A_1 of N_{33} (tampering of measurement data), and the state of attribute A_1 will change from A_1^0 to A_1^2. Similarly, by establishing corresponding logical matching for other elements in the model, the final result of attack modeling on transmitted data can be obtained, which indicates that the attack does not modify the attributes A_1 of measurement data.

By analysis and calculation of equations 4 and 5, it can be seen that in this case of MITM network attack, the attributes of object N_{22} and object N_{33} are modified by the attacker, while the attributes of other nodes and terminal nodes in the communication information network of AVC control system are not changed, and the terminal data transmission of measurement and AVC control system is not affected; by analyzing the network attack model, it can be seen that the attack behavior can only be found by analyzing the attributes of each router in the transmission path, but it is hard to find the attack behavior by analyzing the status of the terminal equipment and detecting packets.

HIL Co-Simulation for the MITM Attack Model

To verify the cyber-attack process and the impact, we built a HIL co-simulation platform to emulate the real cyber-attack on a virtual AVC control system.

Implementation of the MITM Attack

As shown in Figure 7, the HIL co-simulation platform consists of power simulator, communication simulator, power control center, attacker, and routers which work as both the communication equipment and the HIL interface to connect attacker and simulators. The DIgSILENT Power Factory is used as power simulator, where the IEEE 39-bus model (as shown in Figure 8) is used as physical power system to simulate AVC function; the AVC control function is coded with C++ which collects the power system status, calculates the control values, and sends the control signals to the related power nodes in power simulator every 5 seconds; the communication simulation software QualNet is used to build and simulate a virtual communication network, which runs in real time, and provides the interface for external devices, by which the real-life packets can be caught and forwarded in the virtual network; attacker is a program running on another computer, which can change the contents of communication packets; as the HIL interface, routers work as a bridge to connect power simulator, communication simulator, power control center and attacker together, and the attack strategy and process can be emulated on them.

In the platform, the network object N_{11}, N_{22} and N_{33} is separately related to Router1, Router2 and Router3, and the other network object is modeled in the communication simulator, as shown in Figure 7. Router1 and Router2 work as hardware interface to forward the packets from power simulator to the communication simulator QualNet; Router3 works as the interface for emulating attack process by configuring the router's access control list (ACL) which blocks the regular data transmission and forwards data to the attacker. When HIL co-simulation begins, it will show the attacker how to exploit the weakness and attack the virtual AVC control system.

During the co-simulation, the DIgSILENT sends the power status data to the AVC control center; the control center sends voltage adjustment command to generator G_3 and G_4 via the routers and virtual network. The regular path for measure data forwarding to the AVC control center is from Router1 via Router2 to the virtual network built in QualNet. However, in the scenario of the MITM attack, after the attacker attacked the Router2 via the Router3, changed the routing rules, and created the by-pass traffic focusing on the specific power node measurement data to fudge the measurement data; after the packets of fudged the measurement data passing though the virtual network, they are transmitted to the AVC control center; then, the AVC control center makes a wrong control decision based on the fake measurement data, and sends the control packets to the communication simulator; passing by the virtual network and router, the control packets forward to the power simulator to continue the power simulation.

Result of Simulation

Case 1: Normal operation. Case 1 is the normal operating scenario. After power system failure happens, AVC adjusts voltage magnitudes of every generator with the time interval of 5 seconds. The voltage adjustment command is sent out to generator G_3 and G_4. If the status of Router1 and Router2 is normal, the measurement data of voltage of bus 19 can be correctly transmitted, and the voltage adjustment can be properly executed. The simulation result of voltage magnitude of bus 19 is the green curve shown in Figure 9.

Case 2: Impact of MITM attack. Case 2 is MITM attack scenario. When the attacker changed the routing path of the Router2 and created a by-pass traffic focusing on the measurement data of voltage of bus 19, the attacker can intercept the measurement data, buffer it and resend it in the next measurement data transmission cycle. As the result, the AVC control gives false control, and the voltage adjustment in G_3 and G_4 cannot be executed properly. The simulation result of voltage magnitude of bus 19 is the red curve shown in Figure 9.

Discussion

With the HIL co-simulation platform, the MITM attack can be emulated. The attack process and the status change of real network equipment will be displayed, as well. By analyzing the attack process, it can be found that since the attacker does not directly attack the measurement equipment and control center, but attacks the equipment in the communication link with relatively weak security, the attack behavior is relatively stealthy, and it is difficult to find the attack through the security defense equipment installed in the terminal of the communication system. Therefore, when modeling the cyber-attack, the network topology should be considered, and each node in the communication system should be modeled.

Conclusions

This paper presents a correlated matrix based object-oriented modeling method for network attack analysis, which realizes the modeling of network attack method, attack path, attack steps, and the propagation path of attack behavior in communication and information network. In addition, this method benefits computer by building models fast and efficiently for the large and complex communication networks and network attacks. The comparison of the mentioned modeling methods is shown in Table 1. Based on this modeling method, an attack case of MITM attack on the measurement data of AVC control system is analyzed, which indicates the usage and advantages of this modeling method. Finally, we build a HIL co-simulation platform to emulate the MITM attack process and study the impact on the power system. As the method proposed in this paper has good scalability, it also has some deficiencies, as follows.

1) Through the correlated matrix, it is difficult to directly display the attack behavior and its impact;
2) The structure of correlated matrix is relatively large, and its construction is not well-regulated and universal;

3) This modeling method just shows the cyber-attack model, but the probability of attack discovery and defense is not represented.

And we plan to do the following aspects to further improve the method:

1) Further research for finding the potential attack behavior or evaluating the weak link of the system according to the attack model;
2) Further improvement for the construction method and operation rules of matrix model to make it more expressive and universal;
3) Further research on the "premise and consequence" method to design a matrix model of multiple preconditions;
4) Further research for the representation method of "time and probability" to realize the modeling and calculation for the probability of attack discovery.

References

1. Li X, Wang W, Wang H. A novel bi-level robust game model to optimize a regionally integrated energy System with large-Scale centralized renewable-energy Sources in Western China. Energy. 2021; 228: 120513.
2. Liu CC, Stefanov A, Hong J, Panciatici P. Intruders in the grid. Power & Energy Magazine IEEE. 2012; 10: 58-66.
3. Zhao J, Wen F, Xue Y, Z Dong. Modeling analysis and control research framework of cyber physical power systems. Automation of Electric Power Systems. 2011; 35: 1-8.
4. Tong H, Ni M, Manli Li, Lili Zhao. Flexible hardware-in-the-loop testbed for cyber physical power system simulation. IET Cyber-Physical Systems: Theory & Applications. 2019; 4: 374-381.
5. Lu J, Huang L, Wu S. An attack tree approach for network attack modeling. Computer Engineering and Applications. 2003; 39: 160-163.

6. Ding M, Li X, Zhang J. Effect of scada-oriented cyber attack on power system reliability. Power System Protection and Control. 2018; 46: 37-45.
7. Wang GY, Wang HM, Chen ZJ, Xian M. Research on computer network attack modeling based on attack graph. Journal of National University of Defense Technology. 2009; 31: 74-80.
8. Wang Y, Gao K, Zhao T, Qiu J. Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph. Proceedings of the CSEE. 2016; 36: 1490-1499.
9. Luo Z, Yang X, Liu J, Xu R. Network intrusion intention analysis model based on Bayesian attack graph. Journal on Communications. 2020; 41: 160-169.
10. Li J, Ling X, Li C, Li Z, Yang J, et al. Dynamic network security analysis based on Bayesian attack graphs. Computer Science. 2022; 49: 62-69.
11. Steffan J, Schumachar M. Collaborative attack modeling. Conf. 2002 Acm Symposium on Applied Computing. Madrid, Spain. 2022.
12. Lin ZZ, Wen FS, Yung CC, Po WK. Applications of petri nets in power systems. Proceedings of the Chinese Society of Universities for Electric Power System and Automation. 2007; 19: 57-66.
13. Li B, Lu R, Choo KKR, Wang W, Luo S. On reliability analysis of smart grids under topology attacks: a stochastic petri net approach. ACM Transactions on Cyber-Physical Systems. 2018; 3.
14. Sinha A, Mohandas M, Pandey P, Vyas OP. Cyber physical defense framework for distributed smart grid applications. Frontiers in Energy Research. 2021; 8: 621650.
15. Eckmann, Steven T, Vigna, Giovanni, Kemmerer. Statl: an attack language for state-based intrusion detection. Journal of Computer Security. 2002; 10: 71-104.
16. Vigan G, Kemmerer RA. Netstat: a network-based intrusion detection system. Journal of Computer Security. 1999; 7: 37-71.
17. Zhu J, Xu H, Pan A. An attack knowledge model based on object-oriented technology. Journal of Computer Research and Development. 2004; 41: 1110-1116.

18. Ma Y, Wang LG. Attack graph construction method based on intelligent state transition and permission improvement. Computer Science. 2013; 40: 156-158.
19. Prabha S, Anitha R. Mitigation of application traffic DDoS attacks with trust and AM based HMM models. International Journal of Computer Applications. 2010; 6: 26-34.
20. Zhou D, Zhang H, Zhang S, Hu X. A DDoS attack detection method based on hidden Markov model. Journal of Computer Research & Development. 2005; 42: 1594-1599.
21. Wang GY, Wang HM, Chen ZJ, Xian M. Research on computer network attack modeling based on attack graph. Journal of National University of Defense Technology. 2009; 31: 74-80.
22. Huang B, Li Y, Zhan F, Sun Q, Zhang H. A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks. IEEE Transactions on Industrial Informatics. 2002; 18: 880-890.
23. Rumbaugh BJ, Blaha MR, Lorensen W, Eddy F, Premerlani W. Object-oriented modeling and design. Upper Saddle River: Prentice Hall. 2004.
24. Li M, Ni M, Xue Y, Chen X, Ding W. Hybrid Calculation Architecture of Cyber Physical Power System Based on Correlative Characteristic Matrix Model. Proc. Int. Conf. 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER). Tianjin, China. 2018.

Supplementary Materials

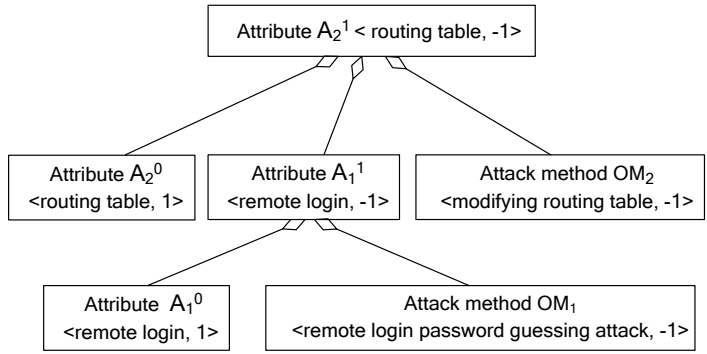

Figure 1: The diagram of object-oriented method for the cyber-attack modeling.

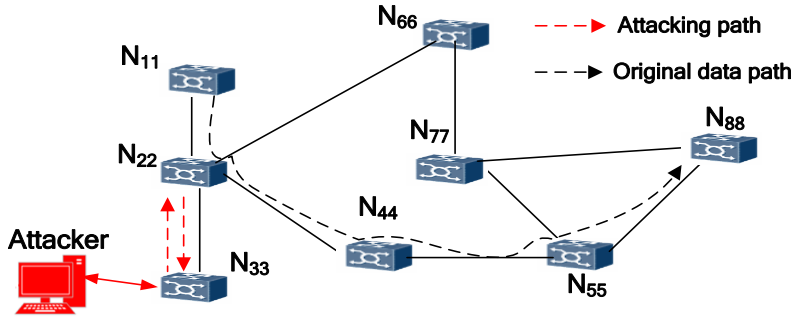

Figure 2: The topology of communication network.

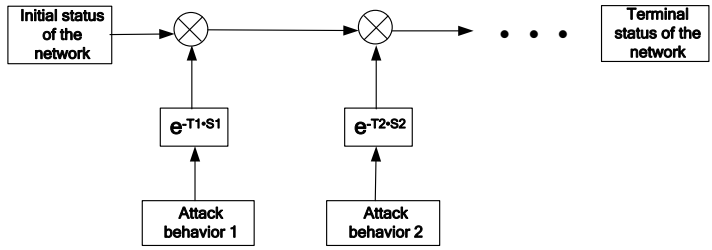

Figure 3: The diagram of cyber-attack model.

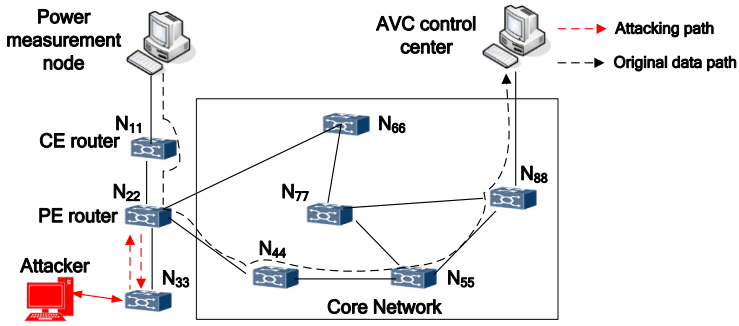

Figure 4: The topology of communication network.

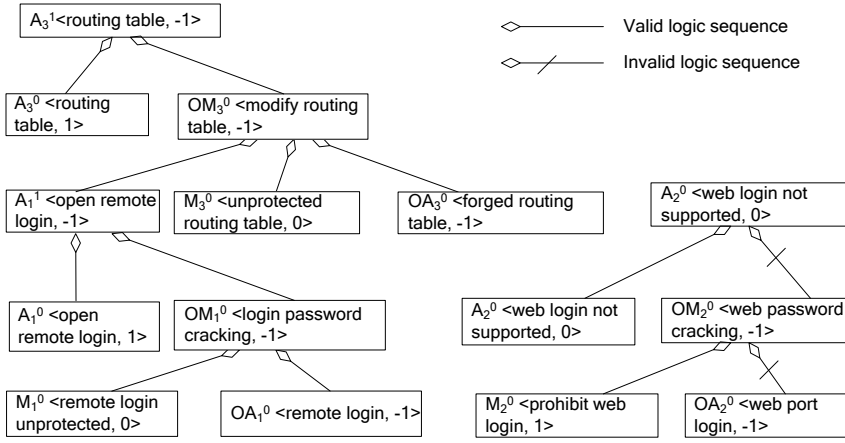

Figure 5: The diagram of logical matching method for the matrix of N_{22}^0 and ON_{22}^0.

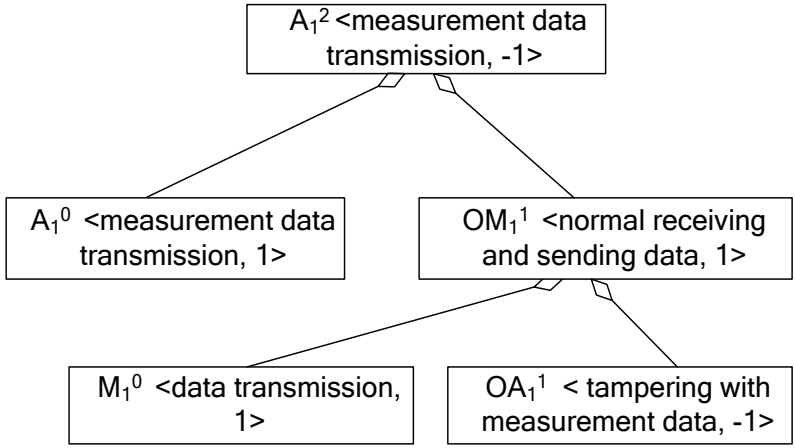

Figure 6: The diagram of logical matching method for the matrix of N_{33}^0 and ON_{33}^1.

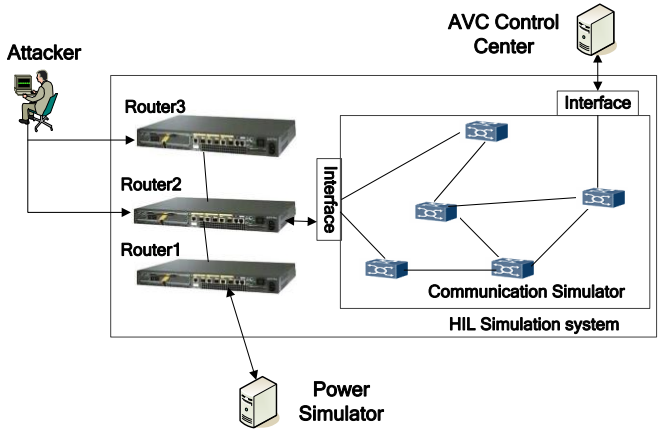

Figure 7: The architecture of co-simulation system for the MITM attack.

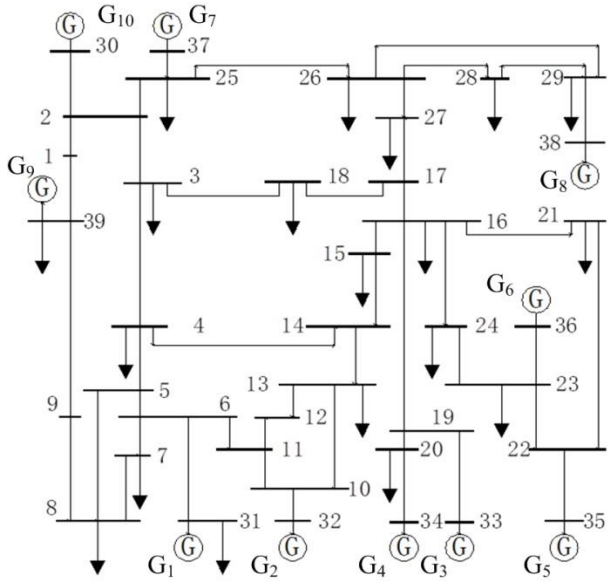

Figure 8: Topology of IEEE 39-bus system.

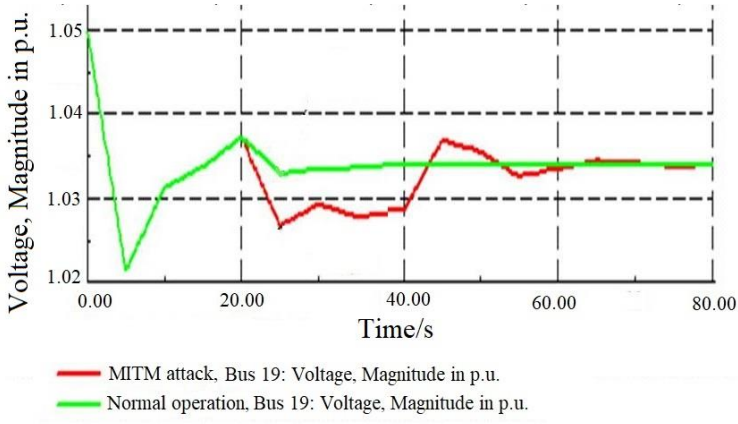

Figure 9: Result of simulation.

Table 1: Comparison of modeling method.

Modeling method	Description of network topology	Description of changes of nodes status	Description of nodes weakness	Description of attack dynamic behavior	Description of attack propagation path
Attack tree model	None	None	None	None	None
Attack graph model	None	None	None	None	None
Attack network model based on Petri Net	Partial	None	None	Yes	No Partial
Network Attack Language	None	Partial	Partial	Partial	None
State transition graph modeling	None	Yes	Partial	Yes	Yes Partial
Correlated matrix based object-oriented model	Yes	Yes	Yes	Yes	Fully displayed